

# **Pharmacy Operational Updates**

## **Multi - DEA Pharmacy Enhancements**

**PSO\*7.0\*545**

**PSJ\*5.0\*372**

**OR\*3.0\*499**

## **Deployment, Installation, Back-out, and Rollback Guide**



**June 2023**

**Department of Veterans Affairs**

**Office of Information and Technology (OIT)**

## Revision History

Date	Version	Description	Author
June 2023	1.0	Initial Version	REDACTED

# Table of Contents

<b>1. Introduction</b>	<b>1</b>
1.1. Purpose	1
1.2. Dependencies	1
1.3. Constraints	2
<b>2. Roles and Responsibilities</b>	<b>3</b>
<b>3. Deployment</b>	<b>4</b>
3.1. Timeline	4
3.2. Site Readiness Assessment	4
3.2.1. Deployment Topology (Targeted Architecture)	4
3.2.2. Site Information (Locations, Deployment Recipients)	4
3.2.3. Site Preparation	5
3.2.3.1. DEA Migration	5
3.2.3.2. DEA Web Server Configuration Verification	6
3.3. Resources	6
3.3.1. Hardware	7
3.3.2. Software	7
3.3.3. Communications	7
3.3.3.1. Deployment/Installation/Back-out Checklist	7
<b>4. Installation</b>	<b>8</b>
4.1. Pre-installation Instructions	8
4.2. Platform Installation and Preparation	8
4.3. Download and Extract Files	8
4.3.1. Other Software Files	8
4.4. Database Creation	9
4.5. Installation Scripts	9
4.6. Cron Scripts	9
4.7. Access Requirements and Skills Needed for the Installation	9
4.8. Installation Procedure	9
4.8.1. Installation Procedure: Multi-Build Host File	9
4.8.2. Installation Procedure: ePCS GUI Executable	10
4.8.2.1. ePCS GUI Setup Instructions	10
4.9. Installation Verification Procedure	11
4.10. System Configuration	11
4.11. Database Tuning	11
<b>5. Back-out Procedure</b>	<b>12</b>
5.1. Back-out Strategy	12
5.2. Back-out Considerations	12
5.2.1. Load Testing	13

5.2.2. User Acceptance Testing .....	13
<b>5.3. Back-out Criteria .....</b>	<b>13</b>
<b>5.4. Back-out Risks.....</b>	<b>13</b>
<b>5.5. Authority for Back-out.....</b>	<b>13</b>
<b>5.6. Back-out Procedure .....</b>	<b>13</b>
<b>5.7. Back-out Verification Procedure .....</b>	<b>18</b>
<b>6. Rollback Procedure .....</b>	<b>19</b>
6.1. Rollback Considerations.....	19
6.2. Rollback Criteria .....	19
6.3. Rollback Risks .....	19
6.4. Authority for Rollback .....	19
6.5. Rollback Procedure .....	19
6.6. Rollback Verification Procedure.....	19
<b>7. Appendix A – Acronyms .....</b>	<b>20</b>

### List of Tables

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities ..	3
Table 2: Timeline.....	4
Table 3: Deployment / Installation / Back-out Checklist .....	7
Table 4: Other Software Files.....	8

# 1. Introduction

The Outpatient Pharmacy (OP) software provides a way to manage the medication regimen of veterans seen in the outpatient clinics and to monitor and manage the workload and costs in the OP. When a user enters an Outpatient order through Computerized Patient Record System (CPRS), the information is sent to the OP package, and this information is displayed to the user who finishes this order in the OP package.

The primary benefits to the veteran are the assurance that he or she is receiving the proper medication and the convenience of obtaining refills easily. The clinicians and pharmacists responsible for patient care benefit from a complete, accurate, and current medication profile available at any time to permit professional evaluation of treatment plans. Utilization, cost, and workload reports provide management cost controlling tools while maintaining the highest level of patient care.

## 1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the multi-build host file PSO\_545\_P SJ\_372\_OR\_499.KID containing patches PSO\*7.0\*545, PSJ\*5.0\*372 and OR\*3.0\*499 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

## 1.2. Dependencies

The following Veterans Health Information Systems and Technology Architecture (VistA) patches must be installed at the site:

- PSO\*7.0\*684
- PSO\*7.0\*667
- PSO\*7.0\*441
- XU\*8.0\*688
- XU\*8.0\*689
- PSJ\*5.0\*399
- PSJ\*5.0\*385
- PSJ\*5.0\*411
- OR\*3.0\*371
- OR\*3.0\*405
- OR\*3.0\*467
- OR\*3.0\*580

### **1.3. Constraints**

This release is intended to be installed in a fully patched VistA system. The release consists of a combined multi-patch Kernel Installation and Distribution System (KIDS) build and a graphical user interface (GUI) executable. The combined build is installed on the VistA server and the executable can be placed on individual workstations, VA Applications Consolidated Server (VACS), or on a Citrix server.

This release is 508 compliant and uses the same security measures as VistA. Users will authenticate using either their Personal Identification Verification (PIV) card or their access and verify codes.

## 2. Roles and Responsibilities

**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities**

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	Department of Veterans Affairs (VA) Office of Information and Technology (OIT) Health Services Portfolio (HSP) Patient Care Services (PCS), and Program Management Office (PMO)	Deployment	Plan and schedule deployment	Planning
2	Health Product Support and Field Operations (FO)	Deployment	Determine and document the roles and responsibilities of those involved in the deployment	Planning
3	Field Testing (Initial Operating Capability- IOC), Health Product Support Testing & VIP Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Application Coordinators	Release Deployment	Application Coordinators release patches	Deployment
5	HSP PCS and FO	Deployment	Execute deployment	Deployment
6	OIT, Development, Security, and Operations (DevSecOps) Infrastructure Operations (IO) VistA Applications Division and Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment
7	Facility Area Manager and OIT support, which may be local or regional	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
8	VA OIT, HSP PCS, and the Development Team	Post Deployment	Hardware, Software and System Support	Warranty

### 3. Deployment

The deployment is planned as a national general availability release. The scheduling of test/mirror installs, testing, and the deployment to production will be at the sites' discretion.

A national release is planned after testing has been successfully completed at initial operating capability (IOC) test sites.

Deployment will be performed by the local or regional OIT staff and supported by team members from these organizations: FO and Enterprise Operations. Other teams may provide additional support.

#### 3.1. Timeline

The deployment and installation is scheduled to run for 31 days, as depicted in the master deployment schedule for Pharmacy Operational Updates Optional Release 2.

**Table 2: Timeline**

Task	Start	Finish
National Release	6/26/23	6/26/23
Compliance Period	6/27/23	7/27/23

#### 3.2. Site Readiness Assessment

This section discusses the locations that will install patches PSO\*7.0\*545, PSJ\*5.0\*372, and OR\*3.0\*499.

##### 3.2.1. Deployment Topology (Targeted Architecture)

This release will be deployed to all VistA instances. There is a server component and a GUI executable.

Health Product Support Patch Release of Products and Patches Guide: [Health Product Support Release of Products and Patches Guide](#).

##### 3.2.2. Site Information (Locations, Deployment Recipients)

The IOC sites are:

- Coatesville VAMC (Coatesville, PA)
- Kansas City VAMC (Kansas City, MO)
- Tennessee Valley HCS (Nashville, TN)

Upon national release, all VAMCs are expected to install this patch prior to or on the compliance date. The software will be distributed in FORUM.

### 3.2.3. Site Preparation

#### 3.2.3.1. DEA Migration

The Drug Enforcement Administration (DEA) migration (released and run via post install in required patch PSO\*7.0\*684) must run to completion not more than 7 days prior to installing this release. If the environment check indicates the migration was run more than 7 days prior to the attempted installation of these DEA patches (PSO\*7.0\*545, PSJ\*3.0\*372, and OR\*3.0\*499), a new migration must be run via the DEA Migration Report [PSO DEA MIGRATION REPORT] option, and these patches cannot be installed until the migration completes.

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
Every VAMC (local VistA instance)	Run the DEA Migration within 7 days of installation using the DEA Migration Report [PSO DEA MIGRATION REPORT] option.	Populate the DEA NUMBERS file (#8991.9) and the associated pointer in the NEW DEA#'s multiple field (#53.21) in the NEW PERSON file (#200).	Steps listed below.	DEA credentialing staff, or patch installer

The output of the DEA Migration Report [PSO DEA MIGRATION REPORT] should also be reviewed to determine if there are valid DEA numbers on file that did not migrate due to an exception.

The DEA Migration Report review should include the following steps:

1. Run the DEA Migration Report and import the delimited output into a spreadsheet.
  - a. The message "The DEA Migration was last run on <Month Day Year@<Time>". If this date is less than 7 days before the current date, the DEA Migration has already been refreshed and patch PSO\*7.0\*545 may be installed without performing the remaining pre-installation steps.
  - b. When prompted "Do you want to re-run the DEA Migration?", enter YES.
  - c. When prompted "Are you sure you want to re-run the DEA Migration?" enter YES.
  - d. When prompted "Date/Time to Queue the DEA Migration:" enter the time to queue the migration. The migration may take several hours to complete.
  - e. Enter "^" at the "DEVICE:" prompt to quit. This prompt is related to the migration report output, which is not required as part of the pre-installation for this patch.

**NOTE:** While the migration is running, the DEA Migration Report displays the message "The DEA Migration is currently running. Report data may be incomplete until the migration is finished."

2. Sort the output by the columns indicating recent provider activity (LAST SIGN-ON and/or LAST RX W/IN 3 YEARS columns).
3. Identify DEA numbers that are associated with recent LAST SIGN-ON or LAST RX provider activity and did not successfully migrate.
4. Make a note of the exception(s) associated with each DEA number/provider from the previous step.
5. If possible, resolve the exceptions from the previous step by updating the incorrect data in VistA or by initiating the process to have the DEA update its data.
6. Re-run the DEA Migration using the optional “queue migration” action in the DEA Migration Report option.
7. Verify the DEA numbers from Step three were successfully migrated.

The output of the DEA Migration Report should be captured at the time it is run to document any DEA numbers that could not be automatically migrated. These DEA numbers must be manually updated after the DEA release (this release) is installed.

### **3.2.3.2. DEA Web Server Configuration Verification**

The PSO DOJ/DEA WEB SERVER must be configured correctly prior to installing PSO\*7\*545. If the web server is not configured correctly, it may be difficult to add, edit or remove DEA information associated with individual providers.

Use the Web Server Manager [XOBW WEB SERVER MANAGER] option to check the web server configurations below:

1. Verify PSO DOJ/DEA WEB SERVER is displayed in the “Web Server Name” column in the list of web servers.
2. In the “IP Address or Domain Name:Port” column of the DEA server identified in Step 1, verify the server begins with the characters “prod” if checking a production environment. Non-prod environments should contain a server that begins with the characters “dev”.
3. At the “Select Action:” prompt, enter “CK” to check web service availability.
4. At the “Select Web Server:” prompt, enter the number in the “ID” column associated with the DEA web server identified in Step 1.
5. Verify the status message “PSO DOJ/DEA WEB SERVICE is available” displays. If the status does not indicate the server is available, do NOT install the patch in a production environment and enter a Service Now ticket with the subject “PSO DOJ/DEA WEB SERVICE is not available – PSO\*7\*545”.

Any DEA numbers that could not automatically migrate should be documented. These DEA numbers must be manually updated after the DEA release (this release) is installed.

## **3.3. Resources**

The DEA Pharmacy Enhancement release does not require any special or specific resources other than a functional VistA system.

### 3.3.1. Hardware

There is no specific hardware required other than that which already hosts the VistA system. This is a software enhancement that will not require additional hardware.

### 3.3.2. Software

There is no specific software required other than that which already hosts the VistA system.

### 3.3.3. Communications

For national release, sites will receive communication that the release has occurred, typically this is an Action Item or Bulletin.

Sites will use their internal communications to let their users know about upcoming installations and any associated downtime. This is critical as users can often slow the installation process if they are on the system while installers are trying to get the software installed.

Clinical Application Coordinators (CACs), installers, and other site personnel (as determined by the site) will need to coordinate installation dates and times. In addition, other support personnel may need to be consulted – such as the Citrix support, Client Technologies (if required).

#### 3.3.3.1. Deployment/Installation/Back-out Checklist

The Release Management team will deploy the patches PSO\*7.0\*545, PSJ\*5.0\*372, and OR\*3.0\*499, which are tracked in the NPM in Forum, nationally to all VAMCs. FORUM automatically tracks the patches as they are installed in the different VAMC production systems as described in the previous section. One can run a report in FORUM to identify when the patch was installed in the VistA production at each site, and by whom. A report can also be run, to identify which sites have not installed the patch in their VistA production system as of that moment in time.

Therefore, this information does not need to be manually tracked. The table is included below if manual tracking is desired.

**Table 3: Deployment / Installation / Back-out Checklist**

Activity	Day	Time	Individual who completed task
Deploy	TBD	TBD	TBD
Install	TBD	TBD	TBD
Back-out	TBD	TBD	TBD

## 4. Installation

Prior to installing the DEA multi-build host file containing patch PSO\*7.0\*545, PSJ\*5.0\*372, and OR\*3.0\*499, the migration of active DEA numbers must be completed and the availability of the PSO DOJ/DEA WEB SERVICE

### 4.1. Pre-installation Instructions

**IMPORTANT:** The following steps **MUST** be completed prior to installing the patches.

- 1) Use the DEA Migration Report [PSO DEA MIGRATION REPORT] option to re-run the DEA migration. See Section 3.2.3.1 **DEA Migration** for detailed instructions.
- 2) Verify the DEA Web Server configuration. See Section 3.2.3.2 **DEA Web Server Configuration Verification** for detailed instructions.

### 4.2. Platform Installation and Preparation

The VistA patches in this release should be installed into the test/mirror/pre-prod accounts before the production account as is the normal VistA patch installation standard convention. When installing any VistA patch, sites should utilize the option “Backup a Transport Global” in order to create a backup message of any routines exported with this patch. Post-installation checksums are found in the Patch Description and in FORUM NPM.

The ePrescribing Controlled Substances (ePCS) desktop executable should follow a normal desktop Delphi client installation.

### 4.3. Download and Extract Files

The software for this patch is being released using a host file.

#### 4.3.1. Other Software Files

This release also includes other software.

**Table 4: Other Software Files**

File Name	Contents	Retrieval Format
ePCSDataEntryForPrescriber.ZIP	ePCS Executable	Binary
PSO_545_P SJ_372_OR_499.KID	PSO*7.0*545 PSJ*5.0*372 OR*3.0*499	ASCII

Documentation describing the new functionality is included in this release. Documentation can be found on the VA Software Documentation Library (VDL) at: <https://www.va.gov/vdl/>.

The DEA multi-package build (PSO\_545\_P SJ\_372\_OR\_499.KID) includes several patches that will be installed in the following order:

- PSO\*7.0\*545
- PSJ\*5.0\*372
- OR\*3.0\*499

The DEA files can be downloaded from the appropriate location:

- 1) Download the following files.
  - a) PSO\_545\_P SJ\_372\_OR\_499.KID
  - b) ePCSDataEntryForPrescriber.zip

## 4.4. Database Creation

Database creation is not applicable for this VistA patch.

## 4.5. Installation Scripts

Installation scripts are not applicable for this VistA patch.

## 4.6. Cron Scripts

Cron scripts are not applicable for this VistA patch.

## 4.7. Access Requirements and Skills Needed for the Installation

To install the VistA patches in the host file, the patch installer must be an active user on the VistA system and have access to the VistA menu option “Kernel Installation & Distribution System” [XPD MAIN] and have VistA security keys XUPROG and XUPROGMODE. Knowledge on how to install VistA patches using the items on this menu option is also a required skill.

**IMPORTANT:** The DEA migration must be run no more than 7 days prior to installing this release. If the migration was last run more than 7 days prior to installation, the migration can be re-run using the DEA Migration Report [PSO DEA MIGRATION REPORT] option.

## 4.8. Installation Procedure

### 4.8.1. Installation Procedure: Multi-Build Host File

**Note:** Do not queue the install.

This patch may be installed with users on the system although it is recommended that it be installed during non-peak hours to minimize potential disruption to users. This patch should take less than 5 minutes to install.

Installation Instructions:

- 1) Use the “Load a Distribution” option contained on the “Kernel Installation and Distribution System” menu to load the Host file.
  - a) When prompted to “Enter a Host File: “ enter: *<path where you downloaded the file>*/PSO\_545\_P SJ\_372\_OR\_499.KID
  - b) Choose to run the Environmental Check option when loading the distribution and ensure there are no errors to handle before proceeding.
  - c) Note that after loading the distribution you are directed to use the name “PSO\*7.0\*545” when taking the install action.

- 2) Optionally execute the “Verify Checksums” option on the same menu.
- 3) Backup the install by using the “Backup a Transport Global” option on the same menu.
- 4) Install the bundle of patches by executing the “Install Package(s)” option.
  - a) For this option at the “INSTALL NAME:” prompt, you will need to use the name “PSO\*7.0\*545” as noted in 1.c above.
- 5) When prompted “Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//”, answer NO.
- 6) When prompted “Want KIDS to INHIBIT LOGONs during the install? NO//”, answer NO.
- 7) When prompted “Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//”, answer NO.
- 8) When prompted “Enter the Device you want to print the Install messages. You can queue the install by enter a 'Q' at the device prompt. Enter a '^' to abort the install. DEVICE: HOME//” press <Enter>.

## 4.8.2. Installation Procedure: ePCS GUI Executable

The most common method for making ePCS available to users is placing the ePCS executable on the VACS servers. In addition, the executable may be placed on a Citrix server for remote access.

The ePCS executable (ePCSDataEntryForPrescriber.exe) should be placed in the location used by the site.

### 4.8.2.1. ePCS GUI Setup Instructions

Following are the instructions to set up the ePCS GUI:

- 1) Upon receipt of the file, ePCSDataEntryForPrescriber.zip, save into your **My Documents** folder.
- 2) Open **Windows Explorer**
- 3) Navigate to C:\Program Files (x86)\Vista
- 4) Right-click on C:\Program Files (x86)\Vista
  - a) Choose New -> Folder
  - b) ePCS<Enter>
- 5) Right-click on My Documents\ePCSDataEntryForPrescriber.zip
  - a) Choose Open with -> Windows Explorer
- 6) Drag the following files to the new ePCS folder
  - a) ePCSDataEntryForPrescriber.exe
  - b) borlndmm.dll
- 7) Navigate to the new ePCS folder

- 8) Right-click on ePCSDataEntryForPrescriber.exe
  - a) Send to -> Desktop (create shortcut)
- 9) You will find the new shortcut on your Desktop. Select the new shortcut.
  - a) Right-click
  - b) Select Properties
    - i) In Target text box, append to the end of  
 "C:\Program Files (x86)\VistA\ePCS\ePCSDataEntryForPrescriber.exe"  
 <space>s=<server> p=<port>
    - ii) For example  
 "C:\Program Files(x86)\VistA\ePCS\ePCSDataEntryForPrescriber.exe"  
 s=vaausvipappdev3.aac.va.gov p=9991
  - c) Click Apply
  - d) Click OK
- 10) Double-click the new shortcut to launch the ePCS GUI.

**Note:** To enter data in the ePCS Data Entry for Prescriber application, the user must have the XUEPCSEEDIT key and the option EPCS GUI Context version 2.2.0.0 [PSO EPCS GUI CONTEXT] as a secondary menu. A user cannot have both the XUEPCSEEDIT key and the ORES key. The two keys are exclusive to one another so that the person prescribing is not also the person controlling authorization for prescribing controlled substances.

## 4.9. Installation Verification Procedure

Verify completed VistA installation by comparing the post-install routine checksums against the published checksums in the Patch Descriptions and in FORUM NPM. To verify VistA is configured for the new version of ePCS, use FileMan inquiry to the OPTION (#19) file. When prompted for the option, enter PSO EPCS GUI CONTEXT. Ensure the ePCS version is: 2.2.0.0.

## 4.10. System Configuration

System configuration is not applicable for this VistA patch.

## 4.11. Database Tuning

Database tuning is not applicable for this VistA patch.

## 5. Back-out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings. In the event of a catastrophic failure, the Area Manager may make the decision to backout the patch and rollback any necessary database changes. The Area Manager, working with site personnel, tier 2 product support, and the Development Team will be involved in the decision. However, the Area Manager will make the final decision.

### 5.1. Back-out Strategy

Prior to installing the updated KIDS package, the site/region should have saved a backup of the routines in a mail message using the **Backup a Transport Global** [XPD BACKUP] menu option. The message containing the backed-up routines can be loaded with the “Xtract PackMan” function at the Message Action prompt. The PackMan function INSTALL/CHECK MESSAGE is then used to install the backed-up routines onto the VistA system.

The Development Team recommends that sites log a ticket if it is a nationally released patch; otherwise, the site should contact the Enterprise Program Management Office (EPMO) directly for specific solutions to their unique problems.

Although it is unlikely due to care in collecting approved requirements, Software Quality Assurance (SQA) review and multiple testing stages (Unit testing, Component Integration Testing, User Acceptance Testing) a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after National Release to the Field. The strategy would depend on during which of these stages the decision is made. If during Site Production Testing, unless the patch produces catastrophic problems, a new version of the test patch correcting the defects will be produced, retested and upon successfully passing Development Team testing, resubmitted to the site for testing. If the defects were not discovered until after national release but during the 30 days support period, a new patch will be entered into the NPM on FORUM and go through all the necessary milestone reviews etc. as an emergency patch.

If backing out the Department of Justice (DOJ) DEA enhancements becomes necessary, sites can use the build created by the Pharmacy Operational Updates Development Team to back out the patches and return the system to the pre-installation state. The same team that placed the GUI executable on the systems will need to replace the GUI with the previous version (ePCS 1.0).

### 5.2. Back-out Considerations

It is necessary to determine if a back-out of the DEA patches PSO\*7.0\*545, PSJ\*5.0\*372 and OR\*3.0\*499 is needed, or if issues may be adequately addressed via a new version of the patch (if prior to national release) or through a subsequent patch (if after national release).

A back-out of the patches will require a new test version (if prior to national release) or subsequent patches (if after national release). If the back-out is post-release of patches PSO\*7.0\*545, PSJ\*5.0\*372 and OR\*3.0\*499, the patches should be assigned the status “Entered in Error” in FORUM’s NPM.

### 5.2.1. Load Testing

Load Testing is not applicable for this VistA patch.

### 5.2.2. User Acceptance Testing

User Acceptance is detailed in [Pharmacy Operational Updates Jira project site](#)

## 5.3. Back-out Criteria

The decision to back-out this VistA patch will be made by Health Product Support (HPS), Consolidated Patient Account Center (CPAC) Revenue System Management staff, and the Development Team. Criteria to be determined based on separate and unique factors and will be evaluated upon post-patch installation use of the product.

Because Pharmacy and CPRS DEA functionality is used by clinical staff on a regular basis, backing out the DOJ DEA enhancements should only be considered because of a catastrophic error.

## 5.4. Back-out Risks

Back-out risks include the current state VistA handling of provider DEA registrations, which are not checked for validity against the issuing authority's source data.

## 5.5. Authority for Back-out

Any back-out decision should be a joint decision of the Area Manager, the Business Owner (or their representative) and the Program Manager with input from the HPS Application Coordinator, HPS Support, and the project Development Team. The ultimate responsibility for backing out the DOJ DEA enhancements lies with the Area Manager.

## 5.6. Back-out Procedure

The back-out plan for VistA applications is complex and not a “one size fits all” solution. The general strategy for a VistA back-out is to repair the code with a follow-up patch. The development team recommends that sites log a ticket if it is a nationally released patch.

If it is prior to national release, the site will be already working directly with the Development Team and should contact that team. The Development Team members are identified in the IOC Memorandum of Understanding (MOU). As discussed in section 5.2, it is likely that the Development Team can quickly address issues via a new software version. If the site is unsure whom to contact, they may log a ticket or contact Health Product Support - Management Systems Team.

The PSO\_545\_P SJ\_372\_OR\_499.KID host file contains the build components listed below.

### **PSO\*7.0\*545**

**Patch PSO\*7.0\*545 installs the following routines:**

Routine Name	New/Modified
PSO7E545	New
PSO7L529	Modified

<b>Routine Name</b>	<b>New/Modified</b>
PSO7L684	Modified
PSO7P545	New
PSO7P684	Modified
PSOCLUTL	Modified
PSOCPTRI	Modified
PSODEADD	New
PSODEAED	New
PSODEAMA	New
PSODEAME	New
PSODEARA	New
PSODEARB	New
PSODEARL	New
PSODEARP	Modified
PSODEART	New
PSODEARU	New
PSODEARV	New
PSODEARW	New
PSODEARX	New
PSODEAU1	New
PSODIR	Modified
PSODIR5	New
PSOEPED	New
PSOEPREP	New
PSOEPRPT	New
PSOEPU1	New
PSOEPUT	New
PSOEPUT2	New
PSOEPVER	New
PSOEPVR	New
PSOERXA0	Modified
PSOERXR1	Modified
PSOHLDS1	Modified

<b>Routine Name</b>	<b>New/Modified</b>
PSOHLEXP	Modified
PSOHLSN1	Modified
PSONEW	Modified
PSOORCPY	Modified
PSOORED1	Modified
PSOORFI5	Modified
PSOORNE3	Modified
PSOORNE5	Modified
PSOOTMRX	Modified
PSOPKIV1	Modified
PSOPRVW	Modified
PSOPRVW1	New
PSORENW	Modified
PSORENW0	Modified
PSORENW4	Modified
PSORLST2	Modified
PSORN52C	Modified
PSOUTIL	Modified

**Patch PSO\*7.0\*545 installs the following options in the OPTION file (#19):**

<b>Option Name</b>	<b>Install Action</b>
PSO DEA EDIT DATA	SEND TO SITE
PSO EPCS DEA INTEGRITY REPORT	SEND TO SITE
PSO EPCS DEA MANUAL ENTRY	SEND TO SITE
PSO EPCS DISUSER PRIVS	SEND TO SITE
PSO EPCS EDIT DEA# AND XDATE	SEND TO SITE
PSO EPCS EXPIRED DEA FAILOVER	SEND TO SITE
PSO EPCS GUI CONTEXT	SEND TO SITE
PSO EPCS MANUAL DEA REPORT	SEND TO SITE
PSO EPCS PRINT EDIT AUDIT	SEND TO SITE
PSO EPCS PRIVS	SEND TO SITE
PSO EPCS SET PARMS	SEND TO SITE

Option Name	Install Action
PSO VAMC MBM PHARMACY MODE	SEND TO SITE

**Patch PSO\*7.0\*545 installs the following Protocols:**

Protocol Name	Install Action
PSODEAME ACCEPT AND SAVE	SEND TO SITE
PSODEAME COPY TO VISTA	SEND TO SITE
PSODEAME EDIT VISTA VALUES	SEND TO SITE
PSODEAME MENU	SEND TO SITE
PSODEAME QUIT AND REJECT	SEND TO SITE

**Patch PSO\*7.0\*545 installs the following List Template:**

List Template Name	Install Action
PSO DEA NUMBER MANAGEMENT	SEND TO SITE

**Patch PSO\*7.0\*545 installs the following Parameter:**

Parameter Name	Install Action
PSOEPCS EXPIRED DEA FAILOVER	SEND TO SITE

**Patch PSO\*7.0\*545 installs the following Remote Procedure Calls:**

Remote Procedure Name	Install Action
PSO EPCS ADD DEA	SEND TO SITE
PSO EPCS DEA DUP CHECK	SEND TO SITE
PSO EPCS DEADOBJ	SEND TO SITE
PSO EPCS DEALIST	SEND TO SITE
PSO EPCS DETOX CHECK	SEND TO SITE
PSO EPCS EDIT	SEND TO SITE
PSO EPCS FIELD HELP	SEND TO SITE
PSO EPCS FILE NP SCHED	SEND TO SITE
PSO EPCS FILER	SEND TO SITE
PSO EPCS GET LIST	SEND TO SITE
PSO EPCS LIST NP SCHED	SEND TO SITE
PSO EPCS LIST OPTN DESC	SEND TO SITE

Remote Procedure Name	Install Action
PSO EPCS MBM	SEND TO SITE
PSO EPCS REMOVE DEA	SEND TO SITE
PSO EPCS REPORTS	SEND TO SITE
PSO EPCS SYSTEM DATE TIME	SEND TO SITE
PSO EPCS TOPIC HELP	SEND TO SITE
PSO EPCS VA# DUP CHECK	SEND TO SITE
PSO EPCS VERSION	SEND TO SITE

### **PSJ\*5.0\*372**

Patch PSJ\*5.0\*372 installs the following routines:

Routine Name	New/Modified
PSGOD	Modified
PSGOE42	Modified
PSGOE82	Modified
PSGOE92	Modified
PSGOEF	Modified
PSGOER0	Modified
PSIVCHK	Modified
PSIVEDT	Modified

### **OR\*3.0\*499**

Patch OR\*3.0\*499 installs the following routines:

Routine Name	New/Modified
ORALWORD	Modified
ORBCMA1	Modified
ORCACT01	Modified
ORCDPS1	Modified
ORCDPSIV	Modified
ORCSAVE	Modified
ORDEA	Modified
ORDEA01	Modified
ORDEA01A	Modified

Routine Name	New/Modified
ORDEA01B	Modified
ORWDPS1	Modified
ORWDPS11	Modified
ORWOR1	Modified

**Patch OR\*3.0\*499 installs the following options:**

Option Name	Install Action
OR ZIP CODE MESSAGE	SEND TO SITE
ORW PARAM GUI	SEND TO SITE

**Patch OR\*3.0\*499 installs the following data dictionaries:**

File Number	File Name	Field Number	Field Name	New or Modified
100	ORDER	110	TEMPORARY DEA# STORAGE	New

While the VistA KIDS installation procedure allows the installer to back up the modified routines using the "Backup a Transport Global" action, the back-out procedure for global, data dictionary and other VistA components is more complex and requires issuance of a follow-up patch to ensure all components are properly removed and/or restored. All software components (routines and other items) must be restored to their previous state at the same time and in conjunction with the restoration of the data. Please contact the EPMO team for assistance since this installed patch contains components in addition to routines.

## 5.7. Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented, including verification that new components were removed, and modified components were returned to their pre-patch state.

## **6. Rollback Procedure**

Rollback pertains to data. The data changes in this patch are specific to the operational software and platform settings. These data changes are covered in the back-out procedures detailed elsewhere in this document. Rollback is not applicable to this VistA patch.

### **6.1. Rollback Considerations**

Not applicable.

### **6.2. Rollback Criteria**

Not applicable.

### **6.3. Rollback Risks**

Not applicable.

### **6.4. Authority for Rollback**

Not applicable.

### **6.5. Rollback Procedure**

Not applicable.

### **6.6. Rollback Verification Procedure**

Not applicable.

## 7. Appendix A – Acronyms

**Table 5: Acronyms**

<b>Acronym</b>	<b>Definition</b>
ASCII	American Standard Code for Information Interchange
CPAC	Consolidated Patient Account Center
CPRS	Computerized Patient Record System
DIBRG	Deployment, Installation, Back-out, and Rollback Guide
HPS	Health Product Support
IOC	Initial Operating Capability
KIDS	Kernel Installation and Distribution System
OIT	Office of Information and Technology
PIV	Personal Identification Verification
SQA	Software Quality Assurance
VA	Department of Veterans Affairs
VAMC	Veterans Affairs Medical Center
VIP	Veteran-focused Integration Process
VistA	Veterans Health Information System and Technology Architecture